BULL. AUSTRAL. MATH. SOC. 12F99
VOL. 14 (1976), 479-480. (20H20)

An embedding theorem for fields: Addendum

J.W.S. Cassels

The proof of Lemma 2 in [1] invoked elementary analytic number-theory. I have just realized that there is a proof which is entirely elementary. It is doubtless "well-known" (in the usual technical sense that it appears somewhere in the literature) and it is certainly "well-knowable" in Conway's terminology. However, as it renders the entire argument of my paper elementary, I give it here.

The lemma asserts that if

$$f(X) = f_n X^n + f_{n-1} X^{n-1} + \ldots + f_0 \tag{1}$$

is a non-constant polynomial with rational integral coefficients, then there are infinitely many primes p for which there is an integer b satisfying

$$f(b) \equiv 0 \pmod{p} . \tag{2}$$

If $f_0 = 0$ we can take $b = 0$ for any prime p : so we can suppose that

$$f_0 \neq 0 . \tag{3}$$

Suppose, if possible, that (2) has a solution only for the primes p in the finite set P (possibly empty). Let c be any integer which is divisible by all the $p \in P$. Then

$$f\left(f_0 c\right) = f_0 r , \tag{4}$$

where

$$r = f_n f_0^{n-1} c^n + f_{n-1} f_0^{n-2} c^{n-1} + \ldots + 1$$

Received 5 March 1976.

is prime to c , and, in particular, is not divisible by any $p \in P$.

Since $f(X)$ is non-constant by hypothesis, we may certainly pick c so that $r \neq \pm 1$. Let p^* be a prime dividing r , so $p^* \notin P$. By (4) we have

$$f(b^*) \equiv 0 \pmod{p^*}$$

with $b^* = f_0 c$. This contradicts the assumption that P contains all the primes p for which (2) is soluble and so proves the lemma.

Reference

[1] J.W.S. Cassels, "An embedding theorem for fields", *Bull. Austral. Math. Soc.* **14** (1976), 193-198.

Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge,
Cambridge,
England.